Independent Verification & Validation Program	FedRAMP Guidelines	IVV 09-8 Version: Basic Effective Date: May 23, 2016

DOWNLOADED AND/OR HARD COPY UNCONTROLLED
Verify that this is the correct version before use.

AUTHORITY		DATE
Jeffrey Northey (original signature on file)	IMS Manager	05/23/2016
Keenan Bowens (original signature on file)	Process Owner	05/20/2016

REFERENCES	
Document ID/Link	Title
ISO 17020:2012	International Organization for Standardization: Conformity assessment – Requirements for the operation of various types of bodies performing inspection
IVV QM	NASA IV&V Quality Manual
IVV 16	Control of Records
NPR 1441.1	NASA Records Management Program Requirements
https://www.fedramp.gov/files/2015/03/FedRAMP-SAR-Template-v2.0_1.docx	FedRAMP Security Assessment Report template

If any process in this document conflicts with any document in the NASA Online Directives Information System (NODIS), this document shall be superseded by the NODIS document. Any external reference shall be monitored by the Process Owner for current versioning.

1.0 Purpose

The purpose of this system level procedure (SLP) is to document the activities and responsibilities associated with conducting assessments of cloud systems as a third party assessor organization (3PAO) under the Federal Risk and Authorization Management Program (FedRAMP).

2.0 Scope

This SLP applies to the activities of the 3PAO group within the NASA IV&V Program.

3.0 Definitions and Acronyms

Official NASA IV&V Program roles and terms are defined in the Quality Manual. Specialized definitions identified in this SLP are defined below.

3.1 Impartiality

NASA's IV&V Program bases all of its decisions, recommendations, reports and findings upon objective evidence and criteria, rather than on bias, prejudice or preference for any party.

3.2 Independence

NASA's IV&V Program operates as an impartial third party, and maintains technical, financial, and managerial independence from its customers to the greatest extent possible.

3.3 Conflicts of Interest

NASA's IV&V Program proactively seeks to avoid and/or eliminate all situations in which the aims and/or concerns of the Program or its contractors are at odds with the aims and/or concerns of its customers and/or stakeholders.

3.4 FedRAMP Project Manager

The FedRAMP Project Manager is a NASA IV&V employee who is designated by Program Management to manage FedRAMP projects and provide support to 3PAO group members (e.g., security assessors and technical managers).

3.5 Acronym List

3PAO	Third Party Assessor Organization
FedRAMP	Federal Risk and Authorization Management Program
HVA	High Value Assets
IA	Information Assurance
IMS	IV&V Management System
NID	NASA Interim Directive
NIST	National Institute of Standards and Technology
NODIS	NASA Online Directives Information System
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
QM	Quality Manual
SATERN	System for Administration, Training, and Educational Resources for NASA
SLP	System Level Procedure

4.0 Process

4.1 Impartiality, Independence, and Conflicts of Interest

NASA's IV&V Program, its employees and contractors understand the importance of impartiality and the consideration of any potential conflicts of interest in carrying out its certification activities.

The NASA IV&V Program has infrastructure, policies and procedures to manage impartiality and to ensure that the certification activities are undertaken impartially, and has top management commitment to impartiality. The 3PAO group will analyze, document and address the potential conflicts of interest arising from certification activities. The group is structured and managed so as to safeguard impartiality.

Conflict of interest and objectivity is addressed in contractually binding agreements, so that all certification activities are conducted in an independent and impartial manner.

The NASA IV&V Program, while organizationally a part of NASA, is able to provide independent analysis services to NASA because the Program was created to work independently within the NASA agency. This is accomplished with independent management reporting chains at the organizational and project levels. Organizationally, the NASA IV&V Program is part of the NASA Office of Safety & Mission Assurance and has no direct reporting chains within the NASA organizations that develop NASA products.

The NASA IV&V Program does not intend to provide FedRAMP 3PAO assessment services to other NASA organizations. However, should NASA IV&V become engaged to perform such work, the Program would employ the same independence and impartiality to that work as it does to all of its other services.

4.2 Confidentiality

NASA's IV&V Program, its employees and contractors are bound by ethical and legal codes to protect the confidentiality and privacy of our clients, their organizations, projects, and contractors. We will protect and maintain the confidentiality of all information learned about clients, their organizations, projects, and contractors in the course of providing services to them.

Individuals, accountable under this policy, may not purposefully disclose confidential, sensitive or proprietary information within or outside the organization, except to individuals known to be authorized to receive such information. Such individuals will act with due care to avoid the inadvertent disclosure of such information to anyone else, and to avoid its use for personal gain or the advantage of other organizations or entities.

Further, all individuals participating in the inspection activities of the 3PAO group will keep confidential all information obtained or created during the performance of inspection activities, except as required by law.

The group's policies and procedures are meant to protect the confidentiality, availability and integrity of all data. Additionally, the following items will be addressed in order to protect sensitive information:

1. Safeguard sensitive information coming into our possession from unauthorized use and disclosure.
2. Allow access to sensitive information only to those employees that need it to perform services under contract.
3. Preclude access and disclosure of sensitive information to persons and entities outside of the Program.
4. Train employees who may require access to sensitive information about their obligations to utilize it only to perform the services specified in the contract and to safeguard it from unauthorized use and disclosure.
5. Administer a monitoring process to ensure that employees and contractors comply with all reasonable security procedures, report any breaches, and implement any necessary corrective actions.

Unless prohibited by law, if the NASA IV&V Program intends to place any information about a client in the public domain, the Program will notify the client, in advance, of what information it intends to disseminate, who the information will be provided to and when it plans to disseminate that information.

Should the NASA IV&V Program be required by law or authorized by contractual commitments to release confidential information about any recipient of its inspection services, that recipient shall, unless prohibited by law, be notified of what information was provided and to whom it was provided.

Additionally, any information about a client of the NASA IV&V Program obtained from sources other than the client shall be treated as confidential.

4.3 Position Descriptions

The NASA IV&V Program consists of NASA Civil Service and contractor employees working together as an integrated team. Security assessments will be performed by both government and contractor staff. All inspection activities will be performed by this integrated team – no subcontractors will be used.

While integrated team consisting of government and contractor employees will perform inspection activities and document results, NASA IV&V management (civil servants) hold responsibility for final determination of conformity of the inspected items with requirements. Review and inspection activities related to this are covered in IVV 09-4, *Project Management*, sections 4.4.1, *Deliverable Processing*, and 4.4.2, *Deliverable Distribution*.

The following position descriptions reflect the skills required of a project manager and a security assessor, the two positions necessary for the NASA IV&V Program to conduct FedRAMP 3PAO inspections.

4.3.1 Project Manger

- Performs project management duties involving a major subject matter or functional area consisting of a variety of equipment systems performing various functions and purposes.
- Manages inspection project activities, including budget and/or resource estimates, if applicable.
- Assesses project progress and maintains liaison between the various activities in the inspection work involved in the assignment.
- Investigates alternatives when program changes or compromises must be made.

- Performs additional data systems and analysis work.

4.3.2 Security Assessor

- Applies experience with the selection, implementation, testing, monitoring, and documentation of NIST security controls to provide security assurance and manage risk.
- Performs independent assessments (system and software security vulnerability, threat, and risk assessments) and penetration tests on development and large-scale operational environments.
- Performs full-lifecycle (i.e., Concept to Deployment) Information Assurance (IA) security analyses to ensure the logical and systematic conversion of customer or product requirements into total secure systems solutions that acknowledge technical constraints.
- Performs NIST security control assessments in support of Assessment and Authorization (A&A) / Certification & Accreditation (C&A) processes.
- Performs analysis of systems security and software architecture, system security and software requirements, system and software design, source code, and the developer's unit, build, and systems integration test products.
- Performs functional analysis, timeline analysis, detail trade studies, and requirements allocation and interface definition studies to evaluate compliance of software/systems developer's software security specifications and requirements to the software security NIST standards.
- Performs mentoring and training on IA methodologies/ techniques.
- Develops independent test plans, cases, procedures, and scripts and performs independent testing of safety and mission critical software systems to ensure the system will not do what it is not supposed to do and will respond in a safe and desired manner under adverse conditions.
- Interacts directly with targeted development program personnel providing a suitable interface for the program to gain access to the results of IV&V IA analyses.
- Collaborates with cross-functional teams of security and systems analysts performing assessments and/or verification

and validation analyses.

- Analyzes effectiveness/efficiency of the NASA IV&V program's security analysis procedures and processes, and develops/ recommends improvements.
- Prepares presentations, reports, research, and other contract deliverables related to mission assurance analyses performed.
- Certifications including:
    - General-purpose IT Security and Audit Certifications
    - Specialized IT Security Certifications
    - Vendor-specific Certifications

4.4 Training and Monitoring of Inspectors

Before performing any 3PAO inspections, security assessors and technical managers must complete NASA’s IV&V Cybersecurity Training (NICST). An overview of the training and the training curriculum can be found here. The training and education of each 3PAO security assessor and technical manager will be assessed on an annual basis to ensure that their knowledge and skills are current and adequate to continue performing 3PAO assessments. The results of this assessment will be discussed once per year at the NASA IV&V quarterly management review (QMR). The training log which forms the basis for inspector candidacy is located here.

4.4.1 Inspector Witnessing Plan

The following inspector witnessing plan details how the NASA IV&V Program will ensure that security assessors are adequately trained before conducting an inspection under FedRAMP and how the Program plans to ensure that security assessors maintain an acceptable level of training on an ongoing basis to continue conducting inspections under FedRAMP.

Induction - Mentoring

Security assessors performing inspections for the first time will do so in collaboration with at least one other security assessor or technical manager (a mentor) who has experience performing inspections. This collaboration will serve as a new assessor’s induction period within the 3PAO group. Any individual who is part of the 3PAO group and has participated in prior inspections is eligible to be a mentor to a new team member. The mentor will review the inspection procedures and findings of the security assessor to ensure that applicable requirements were met and any findings are accurate. The mentor will make a recommendation to the project manager that the assessor is either fit to conduct future inspections without mentoring, or requires training to acquire necessary skills and needs further mentoring while conducting inspections.

In addition to the training and mentoring provided during the induction period, the NASA IV&V Program provides continuous training and learning opportunities with regularly scheduled events such as workshops, tech discussions, and external training brought onsite.

Monitoring

Results of inspections will be reviewed by the technical manager to ensure satisfactory performance before delivery of those results to customers. The project manager responsible for each inspection will observe the security assessor(s) conducting the inspection as the inspection is taking place. This observation will consist of a review of ongoing analysis to ensure that the assessors are following the procedures necessary for the inspection. The project manager will also review the results of the inspection as documented in a report by the assessor(s). After review of this report, the project manager will evaluate the quality of the inspection by the assessor(s) and recommend any training that is needed based upon this evaluation.

Four-Year Witnessing

Each inspector performing 3PAO inspections for the NASA IV&V Program will be witnessed performing an inspection at least once every four years by a 3PAO project manager or technical manager. To ensure that this witnessing occurs, the Program will utilize NASA’s training management platform, SATERN, to record completion of inspector witnessing. SATERN enables each employee to capture the date of each witnessing event, and is capable of reminding employees when they have an upcoming witnessing requirement. Each time an inspector is witnessed, their SATERN account will be updated with the date of the last witnessing event, which will set the time until their next required witnessing to four years from the date of the employee's last witnessing event. Reminders will be provided to employees by the SATERN system when their next required witnessing is one year away. Additional reminders will be provided as necessary at intervals during that last year.

4.5 3PAO Group Composition

The selection of new 3PAO group members will be determined by a combination of need and resource availability. The list of individuals available to serve on the NASA IV&V 3PAO group can be found on Confluence here. The current list of 3PAO group members is:

Richard Brockway – Technical Manager
Brandon Bailey – Deputy Technical Manager
Adam Alley – Security Assessor
Brad Roeher – Security Assessor

Individuals on this list have completed all training required to perform 3PAO assessments (see section 4.4, *Training and Monitoring of Inspectors*), and are authorized to conduct these assessments for IV&V.

4.6 Conducting Inspections

The NASA IV&V Program will utilize the standards and requirements of the FedRAMP program to conduct all inspections. Any observations or data obtained during inspections shall be recorded in the FedRAMP Security Assessment Report as soon as practical. Any calculations or data transfers occurring during the process of inspection shall be subject to appropriate checks to ensure their accuracy and completeness. All items inspected shall be uniquely identified before they are inspected. In addition if inspectors identify any abnormalities with items to be inspected, the inspector shall notify the client before proceeding if there is any doubt as to the suitability of the item(s) for inspection.

The Program uses a standard image and configuration managed virtual machines (i.e. ova's) from the start of an assessment that ensure our software versions are all consistent before going on an assessment. Additional information on the standard image of our machines is located here. The Program also has segregation of duties to ensure that not all assessors are admins on the laptops. This way, only certain people can perform updates of the software. Any new or updated tools for use during 3PAO assessments are evaluated for their security suitability by NASA Headquarters before they are deployed to our machines.

In the event that the 3PAO group identifies a misconfiguration of our test assets or discovers an error in our assessment, we will contact the customer immediately and resolve the issue. If additional tests are needed to gain assurance on the security posture of the asset then we will perform those tests. For example, if Nessus was deemed to be out of date before the assessment, then we would update Nessus and rescan the necessary asset. Due to the image and virtual machine approach, we are confident that the configurations of the tools will be consistent and accurate and yield consistent results.

4.6.1 Inspection Scoping

To perform an assessment of massive networks/cloud offerings, the assessment team must properly scope and sample the customer’s cloud offerings. Under most circumstances the assessment team will not be able to assess every machine within the cloud architecture. Therefore, a risk based-assessment and sampling will be performed to determine the High Value Assets (HVA).

Items to consider when scoping:

- With assistance from the customer, the team will collect configuration files on network devices (layer 2/3) to design a model of the network architecture.
- Analyze the network architecture to determine the network exposure of assets.
- For example, items with a large attack surface (i.e. internet exposed) will need to be included in the sampling.
- Analysis of credentialed vulnerability scan data.
- Based on operating system and function perform analysis to determine if a sampling of operating systems and functions can be performed to represent the security posture of the customer.
- Compare scan results per function and operating system to understand if sampling of hosts will accurately represent the

security posture. For example, compare 10 Windows 7 scans (or 10 databases) to see if identical vulnerabilities were identified.

- Criticality of host based on its function to support the mission needs. Items that may impact the confidentiality, availability, or integrity of the service offered by the customer should be considered as critical and in scope.
- Review necessary documentation to determine patch management, configuration management and system/security architecture.

Considering the network exposure, mission function, and commonality of baseline configuration, the scope of sampling needed can be determined.

4.6.2 Inspection Closeout

After inspection activities are complete, the technical manager for a 3PAO inspection will ensure that an evaluation is conducted of the products and/or services provided to the customer to verify that all of the requirements of the contract have been met.

NASA IV&V will provide reports of inspection results using the most recent version of the FedRAMP Security Assessment Report template from https://www.fedramp.gov/resources/templates-3/. This template will be modified as necessary to conform to all requirements of ISO 17020, *Conformity assessment – Requirements for the operation of various types of bodies performing inspection*.

5.0 Metrics

Any metrics associated with this SLP are established and tracked within the NASA IV&V Program's Metrics Program.

6.0 Records

The following records will be generated or updated and filed in accordance with this SLP and IVV 16, *Control of Records*, and in reference to NASA Procedural Requirements (NPR) 1441.1, *NASA Records Management Program Requirements*.

Record Name	Original	Vital	Responsible Person	Retention Requirement	Location
FedRAMP 3PAO Assessment Report	Y	N	FedRAMP Project Manager	Retire at close of program/project (8/101)	ECM

VERSION HISTORY				
Version	Description of Change	Rationale for Change	Author	Effective Date
Basic	Initial Release	New process	Keenan Bowens	05/23/2016